


Certification concept of the certification body of the German Federal Chamber of Notaries for qualified certificates



Version:

3.0

Date:

07 July 2022

Document history

Version	Comment	Date
1.0	Creation of the document as part of the verification of compliance with the requirements of Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation) by an accredited conformity assessment body.	20 June 2017
2.0	Update due to the conversion of the PKI infrastructure of the certification body of the Federal Chamber of Notaries to a native eIDAS PKI as well as editorial changes as a result of the entry into force of the German Trust Services Act [Vertrauensdienstegesetz - VDG]	18 October 2017
2.1	Update due to new certificate hierarchy	28 February 2018
2.2	Editorial adjustments and update due to further development of the application landscape (application, verification and production system) of the certification authority.	15 August 2018
2.3	Editorial changes as well as adjustments with regard to the Federal Network Agency's (BNetzA) decree pursuant to Section 11 VDG on recognised "other identification methods".	7 June 2019
2.4	Update CA hierarchy	15 June 2020
2.5	Editorial changes as well as extension by contents for the introduction of remote signature pursuant to EN 319 411-2.	9 December 2020
2.6	Review and addition of ECC to certificate profile.	31 May 2021
2.7	Update certificate profile of the certificates for participants	07 December 2021
2.8	Update CA hierarchy	31 March 2022
2.9	Update eIDent with eIDAS token	30 May 2022
3.0	Detailing attribute "countryName" in certificate profile	07 July 2022

Content

1	Introduction.....	8
1.1	Overview.....	8
1.1.1	About this document.....	8
1.1.2	Properties of the PKI of the certification body of the German Federal Chamber of Notaries.....	9
1.2	Name and identification of the document	11
1.3	PKI participant	11
1.4	Use of certificates	11
1.5	Management of the certification concept.....	11
1.6	Definitions and abbreviations.....	12
2	Responsibility for directories and publications.....	13
2.1	Directories	13
2.2	Publication of information on certificates.....	13
2.3	Timing and frequency of publications	13
2.4	Access to the information.....	13
3	Identification and authentication.....	14
3.1	Naming rules.....	14
3.1.1	Types of names	14
3.1.2	Meaningfulness of names.....	14
3.1.3	Pseudonyms.....	14
3.1.4	Rules for interpreting different forms of names	14
3.1.5	Uniqueness of names	14
3.1.6	Recognition, authentication and the role of brand names	15
3.1.7	Test certificates.....	15
3.2	Identification of certificate holders	15
3.2.1	Identification of the applicant	15
3.2.2	Identification in case of extensions and limitations in the certificate.....	19
3.3	Identification and authentication for key renewal requests (re-keying)	21
3.4	Identification and authentication when submitting a revocation request	21
4	Operating requirements.....	22
4.1	Certificate request	22
4.2	Processing of the certificate application	22
4.2.1	Carrying out identification and authentication	22
4.2.2	Acceptance or rejection of the application	23
4.3	Issue of certificates	23

4.3.1	Procedure of the CA in issuing the certificate	23
4.3.2	Notification of the certificate holder about the creation of the certificate	23
4.4	Certificate handover	23
4.4.1	Behaviour during certificate handover	23
4.4.2	Publication of the certificate by the VDA BNotK	24
4.4.3	Notification of third parties about the creation of the certificate	24
4.5	Use of the key pair and the certificate	25
4.5.1	Use of the private key and the certificate by the certificate holder	25
4.5.2	Use of the public key and the certificate by certificate holders.....	25
4.6	Certificate renewal (certificate renewal).....	25
4.7	Certificate renewal with key renewal.....	25
4.8	Certificate change	25
4.9	Revocation and suspension of certificates	25
4.9.1	Conditions for revocation	25
4.9.2	Entitled to revocation	26
4.9.3	Procedure for submitting a revocation request	27
4.9.4	Deadlines for a revocation request	27
4.9.5	Time period for processing the revocation request	27
4.9.6	Methods for checking revocation information.....	28
4.9.7	Frequency of publication of revocation lists	28
4.9.8	Maximum latency for revocation lists	28
4.9.9	Online availability of revocation information.....	28
4.9.10	Necessity for online verification of revocation information	28
4.9.11	Other forms of displaying revocation information.....	28
4.9.12	Special requirements in case of compromise of the private key	28
4.9.13	Suspension of the certificate	28
4.10	Status request service.....	28
4.11	Termination of the certification service	29
4.12	Deposit and recovery of keys	29
5	Non-technical security measures	30
5.1	Structural security measures	30
5.2	Procedural requirements.....	30
5.2.1	Role concept	30
5.2.2	Four-eyes principle	31
5.2.3	Other instructions.....	31
5.3	Personnel concept	31

5.3.1	Qualification, experience and reliability of staff	31
5.3.2	Security check	31
5.3.3	Training and further education.....	31
5.3.4	Appointment, withdrawal and change of roles	31
5.3.5	Requirements for external personnel	32
5.3.6	Sanctions for unauthorised actions	32
5.3.7	Documentation	32
5.4	Logging of monitoring measures	32
5.4.1	Monitoring of access	32
5.4.2	Monitoring of organisational measures	33
5.5	Archiving of documents.....	33
5.5.1	Types of documents.....	33
5.5.2	Retention periods	33
5.5.3	Archive security	33
5.5.4	Data backup of the archive.....	34
5.5.5	Requirements for the time stamps of the archived records	34
5.5.6	Place of archiving.....	34
5.6	Key changeover	34
5.7	Emergency concept	34
5.7.1	Incident handling	34
5.7.2	Recovery of IT systems	34
5.7.3	Recovery after compromise of private CA keys	34
5.7.4	Continuation of operation after compromise or catastrophe.....	35
5.8	Termination of certification operations	35
6	Technical security measures	37
6.1	Generation and installation of key pairs	37
6.1.1	Generation of key pairs	37
6.1.2	Delivery of private keys for certificate subscribers	37
6.1.3	Delivery of the public keys to the CA.....	37
6.1.4	Delivery of the CA public keys	37
6.1.5	Key lengths.....	38
6.1.6	Key parameters and quality control of the parameters	38
6.1.7	Key usage	38
6.2	Private key security and cryptographic module	38
6.2.1	Standards and security measures.....	38
6.2.2	Multi-eye principle for key activation.....	38

6.2.3	Key restoration	38
6.2.4	Key backup.....	38
6.2.5	Key archiving.....	39
6.2.6	Key transfer.....	39
6.2.7	Key storage	39
6.2.8	Activation of private keys	39
6.2.9	Deactivation of private keys	39
6.2.10	Destruction of private keys.....	39
6.2.11	Description of the cryptographic modules	39
6.3	Other aspects of key pair management	39
6.3.1	Archiving the public keys	39
6.3.2	Validity period of keys and certificates	40
6.4	Activation data.....	40
6.4.1	Generation and installation of activation data.....	40
6.4.2	Protection of activation data	40
6.4.3	Other aspects of the activation data	40
6.5	Computer security	40
6.6	Technical control during the life cycle.....	41
6.6.1	Security measures during the construction, development and expansion of IT systems and software components.	41
6.6.2	Safety measures during operation	42
6.7	Network security	43
6.8	Time stamp	43
7	Certificate profiles, revocation lists and OCSPs	44
7.1	Certificate profiles	44
7.1.1	Root CA	44
7.1.2	Participant certificate profile.....	50
7.2	Revocation list profiles	53
7.3	Status query service profiles.....	54
8	Compliance check.....	54
9	Other business and legal regulations	54

1 Introduction

1.1 Overview

1.1.1 About this document

The German Federal Chamber of Notaries is a qualified trust service provider in the sense of Art. 3 lit. 20 of the eIDAS Regulation (EU) No. 910/2014. Trust services offered are qualified certificates for electronic signatures for natural persons (QCP-n-qscd) and qualified electronic time stamps. The use of the qualified certificates requires the use of a qualified electronic signature creation device (**QSCD**).

This is the certification concept of the certification body of the German Federal Chamber of Notaries (**VDA BNotK**) for qualified certificates for electronic signatures (the **qualified certificates** or the **qualified certificate**) in the form of a Certificate Practice Statement (**CPS**) and represents the requirements of the certification body of the German Federal Chamber of Notaries for and the procedure in the issue, administration, revocation and renewal of the qualified certificates it issues. Non-qualified certificates are not covered.

The certification concept refers to the certificate policy of the Certification Body of the German Federal Chamber of Notaries with the OID 1.3.6.1.4.1.41460.5.1.1.2.1.5 as well as the ETSI Normen EN 319 401, EN 319 411-1 and EN 319 411-2. It describes the implementation of the resulting requirements.

This certification concept is published on the website of the VDA BNotK under the following link: <https://zertifizierungsstelle.bnotk.de/veroeffentlichungen>.

The structure of the certification concept is based on the RFC 3647 standard to facilitate comparison with the certification concepts of other trust service providers.

Only the German version of this certification concept is authoritative. In case of discrepancies between the German and the English version of this document, only the German version shall apply.

This certification concept is not legally binding. Instead, the relationship between VDA BNotK and the certificate holder or the relying third party shall be governed exclusively by the contractual provisions or, in the absence of a contractual relationship, by the statutory provisions. Unless expressly stated otherwise, this certification concept does not contain any assurances, guarantees or warranties.

1.1.2 Properties of the PKI of the certification body of the German Federal Chamber of Notaries

PKI for qualified trust services

The qualified PKI of the German Federal Chamber of Notaries consists of a root CA and sub-CAs derived from it. Subscriber certificates are signed by the respective sub-CAs.

RSA algorithm

► Active

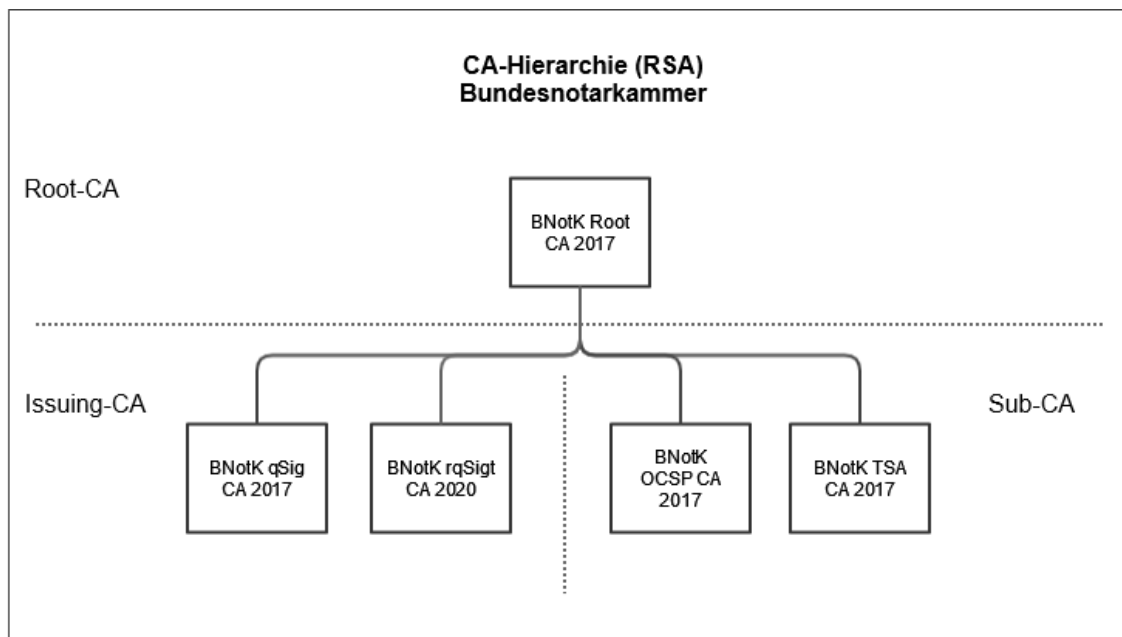


Figure 1: active PKI hierarchy for qualified certificates with RSAPlanned

► Planned

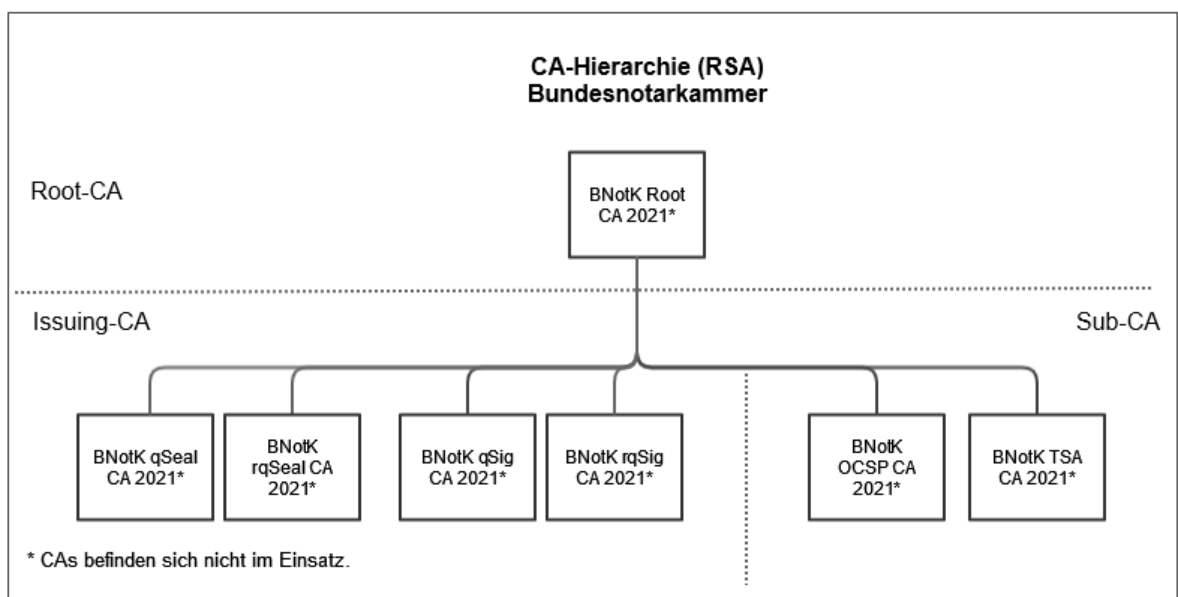


Figure 2: planned PKI hierarchy for qualified certificates with RSA

Elliptic Curve

► Active

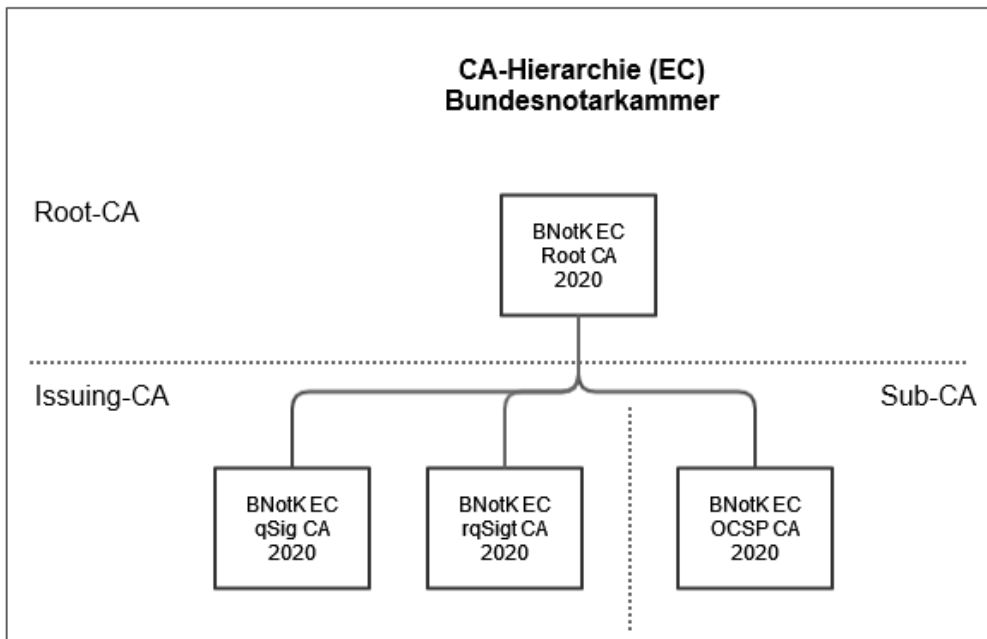


Figure 3: planned PKI hierarchy for qualified certificates with Elliptic Curve

► Planned

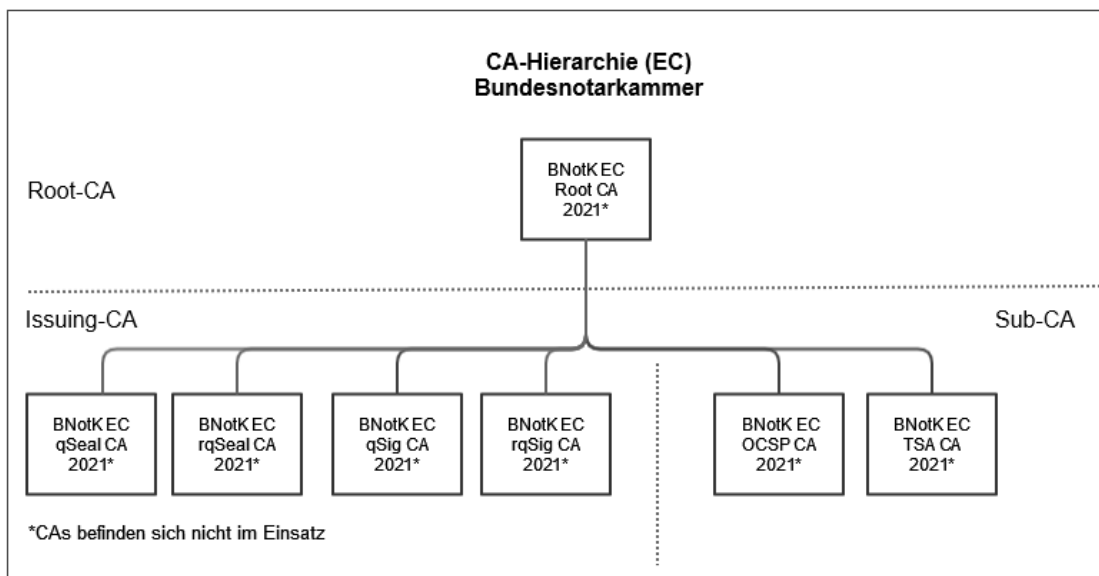


Figure 4: planned PKI hierarchy for qualified certificates with Elliptic Curve

Qualified certificates

The issued end-user certificates comply with the requirements of the eIDAS regulation as well as the following certification level according to ETSI EN 319 411-2:

QCP-n-qscd - Qualified Personal Certificates on Qualified Signature Creation Device.

1.2 Name and identification of the document

Document name: Certification concept of the Certification Body of the German Federal Chamber of Notaries.

Identification (OID): 1.3.6.1.4.1.41460.5.2.1.1.2.3.0

Version: 3.0

1.3 PKI participant

See section 1.3 of the Certification Policy (CP) of the Certification Body of the German Federal Chamber of Notaries.

1.4 Use of certificates

Certificate holders may only use the qualified certificates issued by the VDA BNotK for their own professional purposes. In this respect, they act on their own responsibility. The assessment of whether this certification concept meets the requirements of an application and whether the use of the qualified certificate in question is suitable for a particular purpose is the responsibility of the certificate holder. The VDA BNotK accepts no liability in the event that a certificate holder uses a qualified certificate for other than professional purposes.

A QSCD is required for the use of the qualified certificates.

Furthermore, the certificate holder is subject to the obligations arising from the statutory regulations and, if applicable, to further-reaching or deviating obligations based on individual contractual provisions.

1.5 Management of the certification concept

The Certification Body of the German Federal Chamber of Notaries manages the certification concept. It is reviewed regularly, at least every twelve months, and updated if necessary. The certification concept is reviewed in particular in the event of a change in the laws that are essential for the VDA BNotK and in the event of a change in operational procedures. The head of the Certification Body of the German Federal Chamber of Notaries or, if he is prevented, his designated deputy is responsible. In the event of a change, the amended version is published immediately on the VDA BNotK website. If serious changes to the contents of the certification concept are planned, these will be indicated and published in the repository.

Only the head of the Certification Body of the German Federal Chamber of Notaries or, if he is prevented from doing so, his designated deputy may make changes to the certification concept. In accordance with a corresponding operational instruction, changes are only published with the release of the Head of the Certification Body of the German Federal Chamber of Notaries or, if he is

unable to do so, his designated deputy. The change is indicated by the assignment of a new version number.

The contact person responsible for administration can be reached at the following address:

Zertifizierungsstelle der Bundesnotarkammer
(Certification Body of the German Federal Chamber of Notaries)
attn. Head of the Certification Body
Burgmauer 53
50667 Cologne

Tel.: +49 (2 21) 27 79 35-0

Fax: +49 (2 21) 27 79 35-20

Email: zs@bnotk.de

1.6 Definitions and abbreviations

See section 1.6 of the Certification Policy (*CP*) of the Certification Body of the German Federal Chamber of Notaries.

2 Responsibility for directories and publications

2.1 Directories

See section 2.1 of the Certification Policy (*CP*) of the Certification Body of the German Federal Chamber of Notaries.

The qualified certificates are published under the addresses `ldap://ldap.zs.bnotk.de` and `ldap://ldap.bnotk.de`.

2.2 Publication of information on certificates

The VDA BNotK publishes the following information on qualified certificates issued by it:

- ▶ the qualified certificates, unless the certificate holder has objected to this,
- ▶ the instruction booklet for qualified electronic signatures,
- ▶ the Certification Policy,
- ▶ this certification concept,
- ▶ the PKI Disclosure Statement for qualified certificates.

2.3 Timing and frequency of publications

Subscriber certificates are published immediately after they are issued, provided the subscriber has consented to publication. Revocation lists are not published.

Further regulations are described in the Certificate Policy in Section 2.3.

2.4 Access to the information

See section 2.4 of the Certification Policy (*CP*) of the Certification Body of the German Federal Chamber of Notaries.

3 Identification and authentication

3.1 Naming rules

3.1.1 Types of names

Qualified certificates must contain the name of the certificate holder. Qualified certificates conform to the profile of the standard ITU-T Recommendation X 509. V3 and contain a name composed of several pieces of information.

3.1.2 Meaningfulness of names

The names used are unique (cf. section 3.1.5).

3.1.3 Pseudonyms

At the request of an applicant, the VDA BNotK shall list a pseudonym instead of a name in a qualified certificate. The pseudonym must be unmistakably assigned to the certificate holder and identified as such. Pseudonyms are only assigned once within the user group of the VDA BNotK.

Qualified certificates containing a pseudonym comply with the profile of the ITU-T Recommendation X 509. V3 and contain a name composed of several pieces of information. This is at least the following information:

- ▶ CN (common name) = Common name
- ▶ serialNumber = Serial number

3.1.4 Rules for interpreting different forms of names

See section 7.1 of this document.

3.1.5 Uniqueness of names

The name shall be unique to allow identification of the certificate holder without risk of confusion.

Names shall be composed of at least the following elements:

- ▶ First name
- ▶ Last name
- ▶ Common Name
- ▶ serialNumber (= certificate number)

The serialNumber is assigned uniquely. The possibility of confusion between two persons with the same first and last name is excluded, as the uniqueness is given by the addition of "serialNumber".

3.1.6 Recognition, authentication and the role of brand names

The applicant is responsible for the compatibility of the chosen pseudonym with the rights of third parties, e.g. name, trademark, copyright or other protective rights, as well as with general laws.

3.1.7 Test certificates

The VDA BNotK reserves the right to issue test certificates in exceptional cases, the use of which is necessary for test purposes (e.g. integration, training). The number of test certificates issued must be kept low. Test certificates must be clearly identifiable as such. The test certificates must be clearly marked and recognisable as such, e.g. by the unique expression "TEST" in any organisational designation. For the inclusion of pseudonyms, the specification of the expression "test card" followed by any character string that uniquely identifies the certificate holder in the context of the PKI is required.

3.2 Identification of certificate holders

The VDA BNotK shall uniquely identify persons applying for a qualified certificate. Only the information required to provide the trust services offered by the VDA BNotK is recorded. At a minimum, it is necessary to establish the full name as well as the date and place of birth of the applicant. In addition, the applicant must provide his address and an email address.

Identification shall, in principle, be based on the following documents:

- ▶ Identity card of the Federal Republic of Germany,
- ▶ Identity card or electronic residence permit of the Federal Republic of Germany with electronic ID function,
- ▶ Passport issued to a person with citizenship of a Member State of the European Union or a State of the European Economic Area,
- ▶ Documents or suitable technical procedures with equivalent security for identification as the documents referred to in the preceding paragraphs.

Identification is necessary if the applicant has not yet been identified or if the data on which the identification is based has changed (for example, if the applicant's name has changed).

3.2.1 Identification of the applicant

The identification of the applicant may in principle be carried out using the following procedures:

- ▶ Notarident - identification by notaries;
- ▶ Gerichtident - identification by German courts;
- ▶ Rechtsanwaltskammerident - identification by employees of bar associations;
- ▶ eIDent - identification by means of electronic proof of identity
- ▶ RA-Ident - identification by employees of the RA of the VDA BNotK.

The decision on the choice of the concrete identification procedures offered is incumbent on the respective applicant. However, not all identification procedures are offered with all VDA BNotK products. Identification in the Rechtsanwaltskammerident procedure is only possible, for example, when ordering a beA product and only if the responsible bar association offers this procedure. Identification by means of the RA-Ident procedure is only possible when identifying employees of the German Federal Chamber of Notaries public body.

When entering the application, the applicant must select one of the identification procedures offered to him. Depending on the selection made, the applicant will be informed after the online entry of the application data how to use the selected procedure. At the same time, depending on the selected identification procedure, the applicant will be provided with the appropriate identification documents for printing.

3.2.1.1 Notarident procedure

In the Notarident identification procedure, identification is carried out by a notary with an official seat in Germany.

When identifying the applicant, the requirements of the German Notarisation Act [*Beurkundungsgesetz - BeurkG*], in particular from Section 40 BeurkG, must be observed.

The Notarident procedure includes:

- ▶ Receipt of (i) the application documents (signed or still to be signed) and certification of the applicant's signature or (ii) the data sheet (signed or still to be signed) containing all personal data of the applicant provided during the application and certification of the applicant's signature by the notary public;
- ▶ Preparation of a certified copy of the identification documents used for identification by the notary;
- ▶ Dispatch of the documents by the notary to the RA by post or preparation of an electronically certified copy and dispatch to the RA by electronic means. By post, documents are to be sent directly to the RA in a transshipment envelope, which is to be checked for integrity. The electronic files provided with a qualified electronic signature

of the notary will be securely transferred electronically via EGVP to the RA. The transfer is encrypted end-to-end.

In the Notarident procedure, neither an examination of the application documents nor a briefing of the applicant by the notary takes place.

3.2.1.2 Gerichtident procedure

The identification of the applicant can also be done by the president or director of a German court. The requirements for the certification of signatures by public authorities (Section 34 German Administrative Procedure Act [*Verwaltungsverfahrensgesetz - VwVfG*] or corresponding provisions under Land law) must be complied with in this regard.

In the case of identification by a court, the same standards apply for the control obligations and the formulation of the certification as for identification by the notary within the framework of the Notarident procedure (cf. section 3.2.1.1). The applicant must present one of the documents mentioned in section 3.2. at the time of identification. The relevant information shall be documented by attaching a copy of the identification document used for identification to the card application. The documents are sent in an envelope directly by the certifying body to the RA of the VDA BNotK, who checks it for integrity. The confirmation of professional details obtained from the applicant, if any, shall be enclosed - if required - unless it is sent directly by the certifying body.

3.2.1.3 Rechtsanwaltskammerident procedure

If necessary, the identification of the applicant can also take place on the basis of the identification by an employee of the German Bar Association - e.g. in the case of swearing-in in accordance with Section 12a of the German Federal Lawyers' Act [*Bundesrechtsanwaltsordnung - BRAO*].

The Kammerident procedure includes:

- ▶ Receipt of the signed application documents and checking for correctness of form and content by an employee of the bar association;
- ▶ Photocopying of identity documents or comparison of photocopies handed over by the applicant with the (original) identity document;
- ▶ Identification of the applicant and verification of the identification data on the basis of the identity documents;
- ▶ Scanning of all documents (application documents and identity documents) by an employee of the bar association with the application of at least an advanced electronic

signature. The employee shall confirm with the signature that the scans correspond to the paper original in terms of image and content.

- Transfer of the electronic files provided with the at least advanced electronic signature via a web application by the Bar to the RA. The transfer shall be transport-encrypted.

The managing directors of the bar associations are trained by the VDA BNotK and ensure that only unobjectionable personnel, who are also used for identification within the framework of the swearing-in, participate in the Kammerident procedure.

3.2.1.4 eIDent procedure

In the case of identification by means of electronic proof of identity pursuant to Section 18 German Identity Card Act [*Personalausweisgesetz - PAuswG*] in conjunction with Art. 24 Para. 1 Subclause 2 lit. b of the eIDAS Regulation (EU) No. 910/2014, identification takes place during the online entry of the application data and the transmission thereof into the RA system. Electronic proof of identity is provided by transmitting data from the electronic storage and processing medium of the ID card/ eID-Token via the secure eID infrastructure. Proof of the identification process is documented with the application data.

The certification authority accepts all electronic proofs of identity that have the security level "high" and have been recognized by the European Commission.

3.2.1.5 RA-Ident procedure

Applicants who are employees of the Federal Chamber of Notaries public body can be identified by an RA employee. The online entry of the application data and/or its identification is usually carried out directly at the premises of the applicant or at the premises of the VDA BNotK.

The RA-Ident procedure includes:

- ▶ Receipt of the application documents by the RA employee and checking for correctness of form and content;
- ▶ Photocopying of identity documents or comparison of photocopies handed over by the applicant with the (original) identity document by the RA employee;
- ▶ Identification of the applicant and verification of the identification data on the basis of the identity documents by the RA employee;
- ▶ Signature of the applicant on the last page of the application document;
- ▶ Verification and comparison of the signature executed in the presence of the RA employee with the signature visible in the identification document;
- ▶ Signature of the RA employee on the identification form;
- ▶ Creation and signing of a summary of the identification data by the RA employee;
- ▶ Transfer of the identification form together with the application data and the identification document by the RA employee into the RA system by applying at least an advanced electronic signature.

In order to prevent forged applications from being submitted outside the secure RA environment during the RA-Ident procedure, the RA employee signs each page of the application documents or affixes his/her abbreviation. Afterwards, the application data and identification documents as well as an identification form are scanned by the RA employee with at least an advanced signature and transferred to the RA system. In principle, it can be done from any computer workstation with an internet connection to which a signature card reader and a printer/scanner are connected.

3.2.2 Identification in case of extensions and limitations in the certificate

At the request of an applicant, a qualified certificate may contain information on his power of representation for a third person as well as office- and profession-related or other information on his person (attributes). With regard to the information on the power of representation, the consent of the third person shall be proven; office- and profession-related or other information on the person shall be confirmed by the respective competent body. Qualified certificates containing corresponding attributes shall only be issued if the confirmation of the competent body is available. For this purpose, the applicant shall be provided with a corresponding form to print out following his or her card application, together with the request to forward this to the competent body.

3.2.2.1 Listing of office- and profession-related or other information

If an applicant has applied for the inclusion of an office- and profession-related or other indication as an attribute, the competent body shall confirm that the applicant is entitled to use the office- and profession-related or other indication and shall send the confirmation by post to the RA of the VDA BNotK. The confirming body proves its authorisation by means of appropriate documents (e.g. extract from the commercial register).

The confirmation forms are checked together with the other application documents by the RA employees as part of the application check. In addition, the confirmations are documented.

A special feature applies to obtaining confirmation for the inclusion of notarial attributes. In order to avoid obtaining confirmations for requested notarial attributes in each individual case, VDA BNotK, on the basis of written agreements with the regional chambers of notaries, uses the notarial directory maintained by the German Federal Chamber of Notaries as a trustworthy notarial database when checking requested notarial attributes. In this case, the examination of the admissibility of a requested notarial attribute is carried out in such a way that the application system generally only accepts card applications with a notarial attribute if the corresponding authorisation to use such a notarial attribute already results from the notarial directory when the application is submitted.

3.2.2.2 Listing of a power of representation for a third person

If an applicant has applied for the listing of power of representation for a third person, the consent of the third person must be proved to the VDA BNotK. In the case of a legal person (under public or private law), the representative of the legal person confirms that the applicant has the power of representation applied for and sends the confirmation by post to the VDA BNotK. The representative of the legal entity proves his authorisation by means of appropriate documents (e.g. an extract from the commercial register).

This applies accordingly when applying for the inclusion of the power of representation for a natural person.

3.2.2.3 Admission of a pseudonym

If the applicant applies for a pseudonym and a power of representation is to be included in the qualified certificate, the confirmation must include the consent of the represented person to the inclusion of a pseudonym. The represented person shall be notified of the pseudonym.

If the applicant requests a pseudonym and the inclusion of professional or other information about him in the qualified certificate, consent to the pseudonym must also be obtained from the bodies responsible for such information

3.2.2.4 Restriction of use

The use of the qualified certificate may be restricted generally or financially. The corresponding restriction shall also be made known to the confirming body as part of the confirmation of an attribute.

3.3 Identification and authentication for key renewal requests (re-keying)

A key renewal is carried out by producing a new qualified certificate before the old certificate expires. The data and evidence already checked during the initial identification can be used for this. This requires that the identification data and confirmations on attributes available to the VDA BNotK are complete and accurate. Before the certificate expires, the certificate holder is automatically informed about the procedure for issuing a follow-up certificate. Here, the identity is ensured via the login, e.g. with an existing and valid QSCD. At the same time, the certificate holder receives an overview of the relevant data recorded at the VDA BNotK and is requested to check the data and notify the VDA BNotK of any necessary corrections within a specified period of time (at least four weeks). If the data and evidence available to the VDA BNotK are still complete and accurate, a new qualified certificate will be issued. If the identification data have changed in the meantime, a new application and identification is required.

The new qualified certificate is issued on the basis of the existing contractual relationship with the certificate holder. A change in the General Terms and Conditions requires that these have been effectively included in the contract.

A deviating procedure may be agreed in individual cases if this is consistent with the legal and other requirements.

3.4 Identification and authentication when submitting a revocation request

The VDA BNotK offers the following options for revoking certificates issued by it:

- ▶ by telephone and
- ▶ in writing with a handwritten signature

Identification and authentication is carried out:

- ▶ in the case of a revocation request by telephone, by providing the revocation password,
- ▶ in the case of a written revocation request, by verifying the signature.

4 Operating requirements

4.1 Certificate request

The VDA BNotK issues certificates exclusively to members of the professional groups named in Section 1.3.3 of the Certificate Policy (**CP**) of the Certification Body of the German Federal Chamber of Notaries and within the scope of operating the video communication system in accordance with § 78p BNotO.

The application data is always entered via the online application page of the VDA BNotK. It is not possible to submit an application exclusively in writing. The entry is always made by the applicant himself. The application data is transmitted either via web form or via secure API interface after being called up by an authorized application.

In the course of submitting the application, the applicant agrees to the General Terms and Conditions of the VDA BNotK and confirms that he/she has taken note of the training brochure on qualified certificates. Acceptance of the General Terms and Conditions and confirmation that the applicant has taken note of the brochure is a prerequisite for the conclusion of the contract. The General Terms and Conditions are written in German and will be made available to applicants for download in electronic form together with the training brochure.

Cf. section 3.2 on the transmission of documents used for identification to the VDA BNotK.

The VDA BNotK reserves the right to reject applications for the issue of a certificate.

4.2 Processing of the certificate application

4.2.1 Carrying out identification and authentication

After the online application has been submitted, it is checked by the RA employees in accordance with the four-eyes principle, depending on the identification procedure selected. The check is not carried out until the identification documents and any required attribute confirmations have been received.

The VDA BNotK uses various procedures to identify applicants. In some cases (e.g. in the case of the Notarident or Gerichtident procedure), reliable and competent third parties are entrusted with the identification. Cf. the explanations in section 3.2.

Under certain conditions, applications for qualified certificates can be checked automatically by the RA system. This applies, among other things, to certificate applications submitted using the identification procedure eIDent. In this case, an automatic system check of the application data and the electronic proof of identity is carried out.

The identification and authentication of the applicants as well as the verification of further certificate-relevant data (e.g. information on occupation-related attributes) must be completed before the qualified certificate is issued.

After all application data has been cross-checked and confirmed, the second checking RA employee issues the production release.

4.2.2 Acceptance or rejection of the application

The VDA BNotK will reject an application for a certificate if the application documents are incomplete or incorrect, or if identification documents are incomplete, damaged or incorrect. Applications will also be rejected if the application data does not match identification documents or attribute confirmations.

Applications may also be rejected for the following reasons:

- ▶ Ineligibility of the applicant because he/she is not a member of one of the professional groups listed in section 1.3.3. of the Certificate Policy of the Certification Body of the German Federal Chamber of Notaries,
- ▶ No authorization or permission to transfer application data via API,
- ▶ Expiry of deadlines (as a rule three months) for the proof of data and/or documents.

The VDA BNotK reserves the right to reject applications for other reasons as well.

4.3 Issue of certificates

4.3.1 Procedure of the CA in issuing the certificate

The creation of the certificate, the generation of the key and the personalisation of the QSCD take place on the premises of the VDA BNotK. The actual certificate creation is carried out by the BNotK signing component located in the secure computer centre of the VDA BNotK.

After identifying the applicant and cross-checking the application data with the data available in electronic form, the production process is triggered. This includes the initiation of the key generation, the generation of the certificate, as well as the storage of the certificate on the QSCD.

4.3.2 Notification of the certificate holder about the creation of the certificate

The certificate holder is notified of the creation of his certificate by email or EGVP

4.4 Certificate handover

4.4.1 Behaviour during certificate handover

During certificate handover, a distinction is made between signature cards and remote signatures.

► Signature card

The VDA BNotK offers two variants for the surrender of a certificate for signature cards:

- postal dispatch of the QSCD or
- reloading a qualified certificate onto a QSCD already sent to the applicant.

In principle, the certificate is delivered by handing over the QSCD by post to the applicant's registration address or, in the case of notaries, to their business address. The functionality of the QSCD is checked before dispatch. The applicant must confirm receipt of the QSCD online. After the applicant has confirmed receipt of the QSCD and the PIN letter has been generated, the certificate is activated. The transport PIN and PUK are then sent to the applicant. They are sent by post or electronically via EGVP. By means of this PIN, which must be changed before the first use, the applicant can put the QSCD into operation. The PIN can only be changed successfully if the QSCD has not been tampered with. The individual steps are documented.

In the so-called "reload procedure", the qualified certificate is loaded onto a QSCD available to the applicant. The "reloading procedure" is only offered for selected VDA BNotK products. The prerequisite is that the applicant has a QSCD completely produced with qeS keys and that the registration has been completed. The qualified certificate is transmitted end-to-end in encrypted form to the applicant via a website (dashboard). With the help of a signature application component provided as a web application and a suitable card reader, the qualified certificate is loaded onto the previously sent signature card. When the qualified certificate is loaded onto the QSCD, the qualified certificate is activated. The required transport PIN is encrypted with the non-qualified certificate of the card already delivered and is only decrypted and provided to the user in the course of the reloading process.

► Remote signature

The private key of the certificate holder is generated in the CA of the VDA BNotK and kept for signature generation. The certificate can only be used after prior registration with authentication data uniquely assigned to the certificate holder (2-factor authentication).

4.4.2 Publication of the certificate by the VDA BNotK

The VDA BNotK publishes the certificate if the certificate holder agrees.

4.4.3 Notification of third parties about the creation of the certificate

Third parties who have confirmed details in the qualified certificate concerning the power of representation or office- and profession-related or other details shall be informed in writing about the contents of the qualified certificate and shall be informed about the possibility of revoking the qualified certificate (**Third Parties Entitled to Revocation**). A revocation password shall be set for this purpose.

There shall be no separate notification of the creation of the qualified certificate.

4.5 Use of the key pair and the certificate

4.5.1 Use of the private key and the certificate by the certificate holder

Certificate holders may only use the certificates for professional purposes and, in the case of signature cards, may not export the private key from the QSCD.

4.5.2 Use of the public key and the certificate by certificate holders

The certificates may be used by all certificate holders. However, certificate holders and relying third parties may only rely on the public key and the certificate if the following conditions are met:

- ▶ the certificate is used in accordance with the permitted types of use and any restrictions in the certificate have been observed,
- ▶ the certificate chain can be successfully verified up to a trustworthy root certificate,
- ▶ the validity of the certificate has been confirmed via the status request service (OCSP),
- ▶ all other agreements and other precautions have been observed.

4.6 Certificate renewal (certificate renewal)

Certificate renewal is not offered.

4.7 Certificate renewal with key renewal

The renewal of a certificate with a new key pair based on the certificate data of the original certificate is possible after prior authentication of the certificate holder according to Chapter 3.3. The certificate holder must confirm that the data provided during identification (see Chapter 3.2) is still valid. The current versions of the CP and CPS at the time of renewal apply to the new certificates.

4.8 Certificate change

A subsequent amendment of the certificate by the VDA BNotK is not possible.

4.9 Revocation and suspension of certificates

4.9.1 Conditions for revocation

In the following cases, the certificate is revoked by the VDA BNotK:

- ▶ at the request of the certificate holder, a Third Parties Entitled to Revocation or the BNetzA,
- ▶ if the qualified certificate was issued on the basis of incorrect information regarding Annexes I, III and IV of the eIDAS Regulation,
- ▶ in the event of invalidity of information in the certificate,
- ▶ in the event of termination of the activity as trust service provider if this is not continued by another qualified trust service provider, or
- ▶ if facts justify the assumption that (i) the certificate is forged or not sufficiently forgery-proof or (ii) the qualified electronic signature creation devices used have security flaws.

The VDA BNotK shall also revoke certificates in particular if

- ▶ the contractual relationship has been terminated,
- ▶ the certificate holder's application was made on the basis of a framework agreement and this framework agreement has been terminated or has been terminated for other reasons,
- ▶ the algorithms underlying the procedures used have been broken or if there are reasons to assume that the algorithms underlying the procedures used have been broken,
- ▶ a confirmation that the qualified electronic signature creation device used does not meet the legal requirements is not available or is no longer valid,
- ▶ a legal obligation to revoke exists,
- ▶ the reference authorisation does not exist or has subsequently ceased to exist.

The VDA BNotK is also entitled to revoke a certificate if it is aware that the underlying root certificate or the certificate itself has been compromised or revoked by the competent authority.

Certificate holders are obliged to have issued certificates revoked if

- ▶ the signature card or certificate has been lost, misused or possibly compromised,
- ▶ the information contained in the certificate no longer corresponds to the facts, in particular if its continued use would constitute a breach of professional and/or ethical law or other legal provisions.

If the VDA BNotK learns through a third party that the signature card or certificate of a certificate holder has been lost, misused or possibly compromised, it shall contact the certificate holder. The certificate is not automatically revoked.

If there are several certificates on a signature card, all other certificates (qualified and other certificates) of the respective signature card are automatically revoked if one of the certificates is revoked.

4.9.2 Entitled to revocation

The following persons are entitled to revoke the certificate:

- ▶ the VDA BNotK,
- ▶ the certificate holder,
- ▶ Third Parties Entitled to Revocation,
- ▶ the BNetzA.

Persons to whom the certificate holder or a Third Parties Entitled to Revocation have communicated the revocation password shall also be deemed to be entitled to revoke, provided that they communicate the revocation password to the VDA BNotK.

4.9.3 Procedure for submitting a revocation request

Revocation requests may be made (1) by telephone on: (0800) 3550 400, (2) in writing with a handwritten signature to the following address: Certification Body of the BNotK, Burgmauer 53, 50667 Cologne.

Certificate holders who wish to submit a revocation request by telephone must authenticate themselves by naming the agreed revocation password and providing further personal details. If a certificate holder makes a revocation request by telephone without knowing his revocation password, he must confirm the revocation request by means of a one-time link sent to the email address deposited with the VDA BNotK.

A written revocation request must be signed in person and must clearly identify the certificate to be revoked by providing information on the certificate and certificate holder.

The revocation of the certificate is documented by means of an automatically generated revocation log. Furthermore, the certificate holder as well as confirming bodies for additionally requested attributes are informed about the revocation.

The revocation of a certificate cannot be reversed.

4.9.4 Deadlines for a revocation request

Certificate holders shall have certificates revoked without delay if there are grounds for revocation.

4.9.5 Time period for processing the revocation request

Certificates may be revoked by telephone 24 hours a day, seven days a week via a telephone number set up specifically for this purpose. The revocation of the certificate shall take place immediately.

Written revocation requests are processed quickly in the RA and certificates are revoked within 24 hours.

If the certificate holder or Third Parties Entitled to Revocation so request, the revocation will take place on a specific date. Retroactive revocations are not possible.

4.9.6 Methods for checking revocation information

Revocation information can be requested via the OCSP responder. The address of the service is part of the certificate.

4.9.7 Frequency of publication of revocation lists

No revocation lists are provided for certificates.

4.9.8 Maximum latency for revocation lists

No revocation lists are provided for certificates.

4.9.9 Online availability of revocation information

Revocation information can be requested via the OCSP responder. The address of the service is part of the certificate. Revocation information is available immediately, at the latest within 60 minutes, after revocation of a certificate. The system time of all IT systems involved in the revocation is continuously synchronised with the legally valid time pursuant to the German Units and Time Act [*Einheiten- und Zeitgesetz*].

4.9.10 Necessity for online verification of revocation information

There is no requirement to check revocation information online.

4.9.11 Other forms of displaying revocation information

None.

4.9.12 Special requirements in case of compromise of the private key

None.

4.9.13 Suspension of the certificate

Suspension of the certificate is not possible.

4.10 Status request service

Status requests are made via the OCSP responder. The address of the service is part of the certificate and available 24 hours a day, seven days a week. The status query service is highly available to prevent failure. The VDA BNotK will eliminate failures of the status query service within the existing technical and operational possibilities within 12 hours at the latest.

The integrity and authenticity of the status information shall be protected.

4.11 Termination of the certification service

The contracts may be terminated by the VDA BNotK and the certificate holder in accordance with the contractual agreements concluded between them.

4.12 Deposit and recovery of keys

Deposit of keys is not possible.

5 Non-technical security measures

5.1 Structural security measures

All sensitive data and systems relevant to the operation of the VDA BNotK are housed in physically protected security areas. The protection class meets the requirements for the operation for issuing qualified certificates. Access control mechanisms ensure that no unauthorised persons have access to the secure areas. All accesses, including unauthorised access attempts, are logged. Attempts to defeat the security mechanisms, such as break-ins, theft and vandalism, trigger an alarm. Within the security area, there is additional physical protection of the VDA-BNotK's IT systems and keys. Access to the systems is only possible under the dual control principle. This measure and the additional video surveillance provide additional protection against manipulation and theft. The components of the VDA BNotK are separate from other services of the BNotK. The security measures and the underlying security concept are regularly checked by a recognised testing and confirmation body.

The computer centre has also been tested and certified according to "Trusted Site Infrastructure Level 3 Extended" by TÜV Informationstechnik GmbH.

The audit covers the following assessment aspects:

- ▶ Environment
- ▶ Building construction
- ▶ Fire protection, alarm and extinguishing technology
- ▶ Energy supply
- ▶ Ventilation and air-conditioning systems
- ▶ Organisation
- ▶ Documentation

Level 3 Extended certification corresponds to a high protection requirement, i.e. all critical supply systems (in particular the external network connection) are fully redundant. "Extended" means that all requirements of an assessment aspect of the next higher level have been achieved. The assessment is repeated at regular intervals.

5.2 Procedural requirements

5.2.1 Role concept

The role concept implemented and documented in the security concept provides for a division into operational, advisory, administrative and leading roles. The defined roles include the role of IT security officer, who is also responsible for internal auditing, the role as syslog operator, as DB administrator, as CA administrator and as network administrator, as well as the role of RA employee and lockdown officer. Persons appointed to leading roles must be free from commercial, financial

or other influences likely to significantly affect confidence in the VDA BNotK. All employees are given the roles necessary to perform the job through a defined process. A role exclusion principle guarantees that no single person can make security-relevant changes or issue, delete or revoke certificates without authorisation. The revocation of a role also follows a defined process and is documented.

5.2.2 Four-eyes principle

Security-critical processes must always be carried out in accordance with the four-eyes principle. This is implemented through technical and organisational measures.

5.2.3 Other instructions

VDA BNotK employees are not permitted to remove documents, media (with the exception of laptops) and software containing sensitive data from the security area of the VDA BNotK.

5.3 Personnel concept

5.3.1 Qualification, experience and reliability of staff

The VDA BNotK only employs reliable, qualified personnel. Before taking up work in the security-critical area of the VDA BNotK, their specialist knowledge is checked and training is provided. This also applies to all managerial roles at the VDA BNotK. Training measures are documented. The VDA BNotK ensures that there are no conflicts of interest. Employees of the VDA BNotK must refuse to act in the event of a conflict of interest. In this case, they do not face any consequences under labour law.

5.3.2 Security check

All VDA BNotK employees deployed for certification services must submit a police clearance certificate at regular intervals, at least every two years. For managerial roles, a certificate of good conduct is also filed with the supervisory authority.

5.3.3 Training and further education

All staff receive training before taking up their duties and as required. Follow-up training for staff is usually held annually. In addition, follow-up training is carried out when changes are made to the processes, the technology and the framework conditions for the operation of the trust service, or if these are necessary to impart or maintain the necessary expertise of an employee.

5.3.4 Appointment, withdrawal and change of roles

Role appointments, role withdrawals and role changes are carried out in accordance with established internal procedures and are documented and the corresponding minutes signed by the appointee and appointee.

The head of the VDA BNotK is appointed and dismissed by the President of the German Federal Chamber of Notaries. Other persons who assume managerial or supervisory roles at the VDA BNotK, e.g. the Deputy Head of the VDA BNotK as well as the Security Officer of the VDA BNotK, are appointed and dismissed by the Head of the VDA BNotK. An appointment is only made once the required security review and training have been carried out. The implemented role concept and role exclusion criteria ensure that each person working for the VDA BNotK only receives the access and access rights necessary to perform his role. The appointment is documented, the appointee declares his/her agreement with the role by countersigning the corresponding protocol.

Part of the appointment and dismissal is also the creation or withdrawal of access and access authorisations to technical systems and protected areas. Access and entry authorisations are only granted to the extent required for the corresponding role.

5.3.5 Requirements for external personnel

External personnel working temporarily in the security area will always be accompanied and supervised by authorised staff. The same regulations apply to permanently deployed personnel from other companies as to internal personnel.

5.3.6 Sanctions for unauthorised actions

The VDA BNotK has implemented measures (e.g. the implementation of an internal audit procedure) to control compliance with the established rules and procedures for the proper and secure operation of the certification service. Any violations found are remedied. Unauthorised actions may also have consequences under labour law and criminal law.

5.3.7 Documentation

The following documentation will be made available to staff:

- ▶ the security concept (the parts relevant to the performance of the role),
- ▶ the role concept,
- ▶ Certificate Policy and Certification Concept,
- ▶ the process documentation for the activity in the RA,
- ▶ the company's security policy.

5.4 Logging of monitoring measures

5.4.1 Monitoring of access

All access to and exit from the security areas of the VDA BNotK is logged and stored for an appropriate period of time (see section 5.1). Access by visitors is also logged and must be announced

at least 24 hours in advance when visiting the computer centre. Visitors are always accompanied by authorised staff. Video recordings are also stored in the area of the data centre.

5.4.2 Monitoring of organisational measures

The organisational measures are regularly reviewed by the senior roles of the Certification Body. Changes to organisational measures are appropriately documented in the security concept.

5.5 Archiving of documents

5.5.1 Types of documents

All documents required by law for the complete documentation of the life cycle of the CA and the issued qualified certificates and keys are archived in the form of electronic log data or paper-based. This applies to the life cycle of qualified certificates in particular to the documents arising during registration (see section 3.2) as well as the documents on issuance, acceptance, publication and revocation.

The life cycle of the CA and its systems and keys is fully documented. This concerns, among other things, the issuance, destruction and backup of the keys.

In addition, security concepts, role assignment lists, training documents and procedural instructions as well as other documents relevant to the operation (e.g. the certifications, contracts with service providers, documents on the delivery and storage of the blanks as well as their removal for production, the results of the internal audit, the results of the vulnerability and penetration tests) are archived.

5.5.2 Retention periods

The retention period of the documentation complies with the legal requirements for qualified certificates. The qualified certificates issued by the VDA BNotK are also kept beyond the period of their validity together with the associated revocation information and the associated records in accordance with Article 24 Para. 2 lit. h of Regulation (EU) No. 910/2014 for the entire period of the VDA BNotK's operation.

5.5.3 Archive security

The electronic archive corresponds to the state of the art and guarantees long-term archiving in accordance with TR-ESOR that preserves the value of the evidence. The paper-based documentation is stored in a specially protected area of the VDA BNotK. Only authorised employees have access to the documents. The integrity of the electronic archive is guaranteed by affixing signatures. There is also a back-up to prevent data loss. For long-term archiving, the Evidence Record Syntax is also implemented. Qualified time stamps are used to secure the hash trees created.

Only authorised employees of the VDA BNotK have access to the data. Requests to view the documentation are processed by the RA. For this purpose, the certificate holder must contact the VDA BNotK. The RA employee will provide the certificate holder with copies of his or her documentation for inspection.

5.5.4 Data backup of the archive

The backup of the data is carried out according to the state of the art.

5.5.5 Requirements for the time stamps of the archived records

The system time of the systems responsible for archiving is continuously checked against the legally valid time according to the German Units and Time Act.

5.5.6 Place of archiving

Archiving takes place exclusively at the German Federal Chamber of Notaries.

5.6 Key changeover

If required and within a reasonable time before the validity of the existing certificates expires, new keys are generated and the matching certificates are published. This applies to both end-user and CA certificates.

5.7 Emergency concept

5.7.1 Incident handling

The handling of security-relevant incidents and compromises is documented in the security concept. Responsible for the implementation are the leading roles.

5.7.2 Recovery of IT systems

The IT systems of the VDA BNotK are backed up daily and stored remotely at an external location. Restoring the systems is part of the practised and documented IT processes and is carried out by the persons with the corresponding roles according to the role concept.

5.7.3 Recovery after compromise of private CA keys

If private CA keys are compromised, the affected CA certificates are revoked and the supervisory authority is informed. Depending on the type of compromise, the subscriber certificates generated from the CA may also be revoked in consultation with the supervisory authority. Affected certificate holders are informed about the incident and its consequences. The revocation information can generally be requested via the OCSP responder or, in the event of a compromise of the OCSP responder's certificate, via the Trusted List issued by the BNetzA.

After implementing appropriate measures to prevent future compromises, new CA keys are created according to the corresponding specifications, published and then the issuing of new subscriber certificates is started according to a documented process. The same process takes place when the algorithms used become invalid or when a QSCD confirmation expires or is revoked and also affects the subscriber certificates or their keys.

5.7.4 Continuation of operation after compromise or catastrophe

The responsible persons according to the role concept decide how operation is to be resumed, depending on the type of disaster. Operations should be resumed after 10 working days, provided that the cause of the compromise or disaster has been eliminated. Resumption of operations may be achieved either by reinstallation or restoration according to documented procedures or a combination of both. If required, also at an alternative location. Prior to this, however, it is ensured that appropriate measures are taken to eliminate the causes of the failure or compromise in the future.

5.8 Termination of certification operations

The VDA BNotK has a continuously updated termination plan in which details are laid down in the event of cessation of operations. The aim is to ensure continuity of service and an orderly wind-down.

The VDA BNotK shall notify certificate holders and third parties, including relying third parties and the competent supervisory authority, of the discontinuation of the certification service in good time, but at least two months in advance. In addition, all further contractual relationships with third parties concerning the provision of trust services by the VDA BNotK shall be terminated upon discontinuation.

The VDA BNotK attempts to achieve a takeover of all qualified certificates (including the public keys) by another qualified trust service provider, but cannot guarantee this. The VDA shall also hand over - as far as permissible - its complete documentation to the acquiring trust service provider. At least all records pursuant to Article 24 Para. 2 lit. h) of the eIDAS Regulation as well as in particular all information and documentation on the individual certificate holders for registration, logging of all events of the certificate lifecycle and the source data of the OCSP responder as a database extract are handed over. The information on the qualified certificates is provided by the acquiring trust service provider or by the BNetzA on the basis of export and transfer of the certificate status of all certificates regardless of their status.

If a takeover of the qualified certificates by another qualified trust service provider is not possible, the VDA BNotK revokes all still valid qualified certificates. In this case, the issued qualified certificates are transferred to the trust infrastructure created by the BNetzA. The public keys of the root and CA certificate are transferred to the qualified VDA or BNetzA taking over the certificates and continue

to be held publicly available by the VDA or BNetzA for an appropriate period of time. The private keys of affected CAs and existing backups will be destroyed.

The German Federal Chamber of Notaries has agreed to bear the costs for the takeover of the qualified certificates issued by the Certification Body as qualified trust service provider by another qualified trust service provider or their transfer into the trust infrastructure of the competent supervisory authority as well as the costs for the notification of the certificate holders, the supervisory authority and other third parties.

6 Technical security measures

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

CA keys, OCSP keys and keys for qualified subscriber certificates are always generated in a secure environment on an approved QSCD that has been evaluated according to the Common Criteria specifications and is on the EU list of trusted certified components (see section 5.1). In the process, it is technically ensured for signature cards that the key pair assigned to a specific certificate holder is linked to the QSCD assigned to this certificate holder. Within the scope of card personalisation in the RA, it is automatically checked whether it is the QSCD prescribed for the process with the correct certified parameters.

The keys of the subscriber certificates for remote signatures are also generated and stored on a certified QSCD, the HSM.

New key pairs and certificates are generated in good time before the certificate validity expires to ensure a smooth transition. The process for generating CA keys, the key ceremony, takes place according to the corresponding specifications and is documented. The role concept of the VDA BNotK and the four-eyes principle are applied to key generation. In line with previous VDA BNotK practice, the number of VDA BNotK employees authorised to generate keys is kept as low as possible. An independent auditor accompanies the key generation.

6.1.2 Delivery of private keys for certificate subscribers

► Signature card

The private keys are delivered to the certificate holder on the QSCD (see section 4.4.1). The QSCD must be kept in the certificate holder's immediate possession in a theft-proof manner and must not be handed over to employees or third parties for use.

► Remote signature

The private keys are generated and stored exclusively in an HSM and are not delivered to the certificate holders.

6.1.3 Delivery of the public keys to the CA

The public key is transferred to the CA in encrypted form as part of the certificate creation process.

6.1.4 Delivery of the CA public keys

The CA's public keys are available to PKI participants in the Certification Body's publications.

6.1.5 Key lengths

The recommendations of the SOG-IS Crypto Working Group apply to the key length. Currently, RSA keys with a length of at least 2048 bits are used for subscriber certificates. The CA keys have a length of 4096 bits for RSA and 521 bits for ECDSA (secp521r1).

6.1.6 Key parameters and quality control of the parameters

The key parameters and the QSCDs used are based on the recommendations of the SOG-IS Crypto Working Group or the confirmation documents of the QSCD. Compliance with the specifications is continuously checked by a person responsible for this.

6.1.7 Key usage

The CA keys are used exclusively for signing subscriber certificates, the OCSP keys for signing OCSP requests. The CA and OCSP keys are used in a secure environment (compare section 5.1). The key usage for subscriber certificates is part of the X.509 certificate and may only be used for qualified signatures.

6.2 Private key security and cryptographic module

6.2.1 Standards and security measures

The cryptographic modules used comply with the legal requirements and standards and are operated in the environment required according to the certification of the components (see section 5.1). Access to the components is protected by technical and organisational measures.

The QSCD is kept and operated in a secure area of the VDA BNotK. This ensures that the QSCD cannot be manipulated by third parties.

The certification of the QSCDs in use is checked for up-to-dateness during the entire life cycle. If there is a change in the status of the certification, the effects are analysed and appropriate measures are defined.

6.2.2 Multi-eye principle for key activation

CA keys can only be activated in a technically enforced multi-eye principle involving several roles.

6.2.3 Key restoration

Keys cannot be deposited and thus cannot be restored.

6.2.4 Key backup

There are backups of the private CA keys. The backup, restoration and access to the private CA keys encrypted by the HSM is only possible by authorised persons in a four-eyes principle.

6.2.5 Key archiving

Keys are not archived.

6.2.6 Key transfer

The keys secured by the HSM can be transferred in the four-eyes principle for the purpose of exchanging an HSM.

6.2.7 Key storage

Keys are stored on QSCDs.

6.2.8 Activation of private keys

CA keys and OCSP keys can only be activated in a technically enforced multi-eye principle involving multiple roles. Subscriber certificate keys, CA keys and OCSP keys must be activated by entering the PIN.

6.2.9 Deactivation of private keys

Keys are deactivated when the connection between the application, card reader and QSCD is disconnected or when the QSCD is disconnected from the card reader or when the HSM is disconnected or deactivated, as well as when the application accessing it is stopped. Permanent deactivation occurs after the PIN has been entered incorrectly several times. A limited number of reactivation attempts via a PUK are possible.

6.2.10 Destruction of private keys

Keys are destructed by destroying the chip on the QSCD or by deleting the keys secured on the HSM. EE, CA and OCSP keys are destroyed at the end of their validity.

6.2.11 Description of the cryptographic modules

Only modules certified to apply qualified signatures in accordance with the applicable specifications are used.

6.3 Other aspects of key pair management

6.3.1 Archiving the public keys

The public keys of the subscriber certificates are archived in accordance with the legal requirements (see section 5.5).

6.3.2 Validity period of keys and certificates

The validity period of the key pairs and certificates based on them corresponds at most to the permitted validity for qualified certificates according to the algorithm catalogue of the BNetzA. When the suitability of a deployed algorithm or the deployed QSCD expires, the keys are revoked before the certificate validity expires (see section 4.9).

6.4 Activation data

6.4.1 Generation and installation of activation data

► Signature card

PINs are generated in the secure environment of the RA of the VDA BNotK. Depending on the product, the participant receives his PIN via a printed PIN letter or electronically encrypted for the participant. The mailing is always separate from the delivery of the QSCD. The participant can convince himself of the integrity of the QSCD by checking whether the five-digit transport PIN is still active. The transport PIN can be used to set the effective PIN, which is at least one digit longer.

► Remote signature

The signature creation data required to activate the private key is generated by the subscriber as part of the certificate application and identification process and is firmly linked to the certificate holder by the VDA BNotK.

6.4.2 Protection of activation data

In the case of signature cards, the activation data for participants is stored in encrypted form in a secure computer centre of the VDA BNotK. In the case of remote signatures, the certificate holder himself is responsible for protecting his activation data for the authorisation of the private key.

The activation data for CA keys are only known to the owner of the CA key.

6.4.3 Other aspects of the activation data

In addition to the PIN, a PUK is also part of the activation data for signature cards. The PUK is used to reset the misuse counter if the PIN is entered incorrectly. However, it cannot be used to set a new PIN. The PUK is created, installed and secured in the same way as the PIN.

6.5 Computer security

The VDA BNotK uses various technical and organisational measures to ensure that the IT systems can only be used for the designated purpose and are always operated in conformity with the security concept. The mechanisms include monitoring systems, logging systems, multi-level firewall and access systems, strict network segmentation, strict role separation and personalised accounts,

integrity protection and monitoring of the cryptographic modules used, virus protection, regular penetration tests and audits. The IT systems are operated in a secure environment (see section 5.1), to protect them from unauthorised access, modification and theft. Unnecessary services, programmes and accounts are removed before the IT components are put into operation.

The system time of all IT systems of the VDA BNotK is continuously synchronised with the legally valid time according to the German Units and Time Act.

Access to the systems of the VDA BNotK is only granted after appointment to the corresponding role and is immediately withdrawn upon dismissal (see also section 5.3.4). Access is always via multifactor authentication and is logged. Changes to the security mechanisms and IT systems are made according to a defined process, are documented and can only be carried out using the four-eyes principle. The four-eyes principle is technically enforced and cannot be circumvented. This also applies to the recovery of data. The implemented role concept and role exclusion criteria ensure that each person working for the VDA BNotK only receives the access and access rights necessary to perform his role. For this purpose, a distinction is made in the technical roles between various administrative, operational and auditing roles.

There are working instructions for the employees of the VDA BNotK concerning compliance with the specifications on computer security.

In order to prevent unauthorised persons from gaining access to sensitive data, data carriers are securely deleted before they are reused. Defective data media are destroyed according to a secure procedure.

VDA BNotK employees are responsible for their actions in accordance with the applicable legal provisions.

6.6 Technical control during the life cycle

6.6.1 Security measures during the construction, development and expansion of IT systems and software components.

The VDA BNotK follows the principles of "Security by Design". Before changes, extensions or the construction of new systems, as well as in software development projects, the security requirements are ascertained in order to be able to take them into account in the conception phase. The security requirements are derived from the certification concept, the Certificate Policy, the underlying security concepts and the following sources, among others:

- ▶ legal requirements,
- ▶ manufacturer specifications,
- ▶ best practices,
- ▶ if applicable, technical guidelines of the BSI,
- ▶ other applicable standards, if applicable,

the commissioning of new components, changes to systems and the implementation of fixes follow defined processes. All changes are appropriately documented.

The life cycle ends with the safe disposal of the systems.

6.6.2 Safety measures during operation

The operation of the components and compliance with the specified operating parameters are continuously monitored with the help of a monitoring system. If safety-relevant events are detected, an alarm is triggered. It is ensured that no sensitive data is leaked via this channel. The monitoring data is also used for capacity planning. Furthermore, all security-relevant processes and malfunctions as well as staff access are logged. Logged in this context - insofar as security-relevant - are in particular the start and termination of the IT systems, start and termination of the logging functionality of the relevant IT systems (in particular firewall, database systems, TOE, RA system), system crashes, hardware failures, activities of the firewall and routers as well as access attempts to the PKI system. The corresponding logs are kept in accordance with legal requirements.

Only software from trustworthy sources is put into operation. The integrity of the software is continuously monitored and changes to the system are reported. Security-critical errors are corrected within a reasonable time and security-relevant patches are applied promptly. Patches are not applied if they result in disadvantages and instabilities that are more serious than the benefits of the patch. The non-application of such updates and the reason for this is documented.

Certified components are always operated in accordance with the required operating environment. In addition, an automatic log analysis takes place to detect errors and attempted attacks at an early stage. This measure is supplemented by regular manual checks. In addition to the logs, the audit logs are also checked in particular. Attack attempts, violations of the security rules and messages from the monitoring system are reported to the administrators, who immediately take care of rectifying the error or narrowing down possible security-relevant events. Security-relevant incidents and open security gaps are immediately reported to the VDA BNotK security officer, who evaluates the implementation of all measures necessary to remedy the security incident and then has them implemented if necessary and documents the process. Relevant security incidents are reported to the supervising body within 24 hours. If applicable, persons and companies affected by the security incident are also informed immediately.

Critical vulnerabilities that have not been addressed elsewhere are addressed within 48 hours of their discovery. Based on an assessment of the risk associated with such vulnerabilities, the VDA BNotK will fix them or - if this is not possible with economically justifiable effort in relation to the impact - document why they are not fixed.

All IT systems and software components are always operated in accordance with the manufacturer's specifications.

Data is backed up on hard drives, which are replaced as soon as they become inoperable or may no longer be operated according to the manufacturer's specifications. Data loss due to ageing data media is avoided by storing data redundantly.

The VDA BNotK has (*vulnerability scans*) and (*penetration tests*) carried out regularly, quarterly or annually, by an independent and expert third party or employee of the corresponding specialist department of the German Federal Chamber of Notaries. The results are documented, evaluated by the VDA BNotK and any deficiencies identified are remedied, if necessary.

6.7 Network security

The IT systems of the VDA BNotK are protected by firewalls. The networks of the security area are segmented into different network zones and physically separated from each other by multi-level firewall systems. The IT systems are distributed across the different network segments according to their protection needs and functions. Systems of the same protection requirement and with the same functionality are located in the same zones. The most important systems for the operation of the VDA BNotK, such as the root CA, are located in the zone with the highest protection requirement. A separate network is used for the administration of the IT systems. Separate networks also exist for test environments. The connections and protocols between the segments are limited to the minimum necessary for the functional scope. All other connections are blocked and unauthorised access is logged. The transfer of sensitive data is always encrypted. Communication channels requiring special protection can only be established if the two endpoints authenticate each other. The network environment and the connection of the networks are designed for high availability. To ensure compliance with network and system security, penetration tests are regularly carried out on the externally accessible and internal IP addresses by qualified personnel. The penetration tests are repeated in the event of security-significant changes.

Compliance is monitored on a regular basis.

6.8 Time stamp

The rules on the qualified time stamp service are regulated in the document Time Stamp Policy and TSA Practice Statement of the VDA BNotK.

7 Certificate profiles, revocation lists and OCSPs

7.1 Certificate profiles

7.1.1 Root CA

► Certificate profile RSA

Field (OID)	Description	Value
Version	x.509 version number	V3 (2)
serialNumber (2.5.4.5)	serialNumber of the certificate	[6f b8 e3 d6 dc a1 f6 bb]
Signature algorithm	Identifier (OID) Signature algorithm	SHA512withRSAandMGF1 (1.2.840.113549.1.1.10)
Signature hash algorithm	Identifier (OID) Signature hash algorithm	SHA-512 (2.16.840.1.101.3.4.2.3)
algorithmIdentifier	Identifier (OID) key algorithm	RSA (1.2.840.113549.1.1.1)
Key length	Key length	4096 bits
Issuer		
countryName (2.5.4.6)	Name country issuer	C = DE
organizationName (2.5.4.10)	Name of organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Body
commonName (2.5.4.3)	Name holder	CN = BNotK Root CA 2017
Validity		
UTCTime	Start	e.g. 2017-10-09 08:57:57 UTC

(1.3.6.1.4.1.1466.115.121.1.53)	End	e.g. 2037-10-09 08:57:56 UTC
Holder		
countryName (2.5.4.6)	Name country holder	C = DE
organizationName (2.5.4.10)	Name of organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Body
commonName (2.5.4.3)	Name holder	CN = BNotK Root CA 2017
Extensions		
keyUsage (2.5.29.15)	Purpose	keyCertSign, cRLSign
basicConstraints (2.5.29.19)	Restrictions on the use of the certificate	Type applicant=Certification Body Constraint path length=0
subjectKeyIdentifier (2.5.29.14)	Public key identifier of the holder	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Issuer public key identifier	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Reference to issuer and service for status inquiry	see following elements
calssuers (1.3.6.1.5.5.7.48.2)	URL to exhibitor info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL to the OCSP service	http://ocsp.zs.bnotk.de/eqsig

► Certificate profile ECC

Field (OID)	Description	Value
Version	x.509 version number	V3 (2)

serialNumber (2.5.4.5)	serialNumber of the certificate	[6f b8 e3 d6 dc a1 f6 bb]
Signature algorithm (1.2.840.10045.4.3.4)	Identifier (OID) Signature algorithm	SHA512WITHECDSA
Key length	Key length	521 bits
Issuer		
countryName (2.5.4.6)	Name country issuer	C = DE
organizationName (2.5.4.10)	Name of organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Body
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK Root CA 2017
Validity		
UTCTime	Start	Certificate valid from
	End	Certificate valid until
Holder		
countryName (2.5.4.6)	Name country holder	C = DE
organizationName (2.5.4.10)	Name of organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Body
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK Root CA 2017
Extensions		

keyUsage (2.5.29.15)	Purpose	keyCertSign, cRLSign
basicConstraints (2.5.29.19)	Restrictions on the use of the certificate	Type applicant=Certification Body Constraint path length=0
subjectKeyIdentifier (2.5.29.14)	Public key identifier of the holder	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Issuer public key identifier	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Reference to issuer and service for status inquiry	see following elements
caIssuers (1.3.6.1.5.5.7.48.2)	URL to exhibitor info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL to the OCSP service	http://ocsp.zs.bnotk.de/eqsig

► Sub-CA Certificate Profile RSA

Field (OID)	Description	Value
Version	x.509 version number	V3 (2)
serialNumber (2.5.4.5)	serialNumber of the certificate	e.g. [6f b8 e3 d6 dc a1 f6 bb]
Signature algorithm	Identifier (OID) Signature algorithm	SHA512withRSAandMGF1 (1.2.840.113549.1.1.10)
Signature hash algorithm	Identifier (OID) Signature hash algorithm	SHA-512 (2.16.840.1.101.3.4.2.3)
algorithmIdentifier	Identifier (OID) key algorithm	RSA (1.2.840.113549.1.1.1)
Key length	Key length	4096 bits
Issuer		
countryName (2.5.4.6)	Name country issuer	C = DE
organizationName (2.5.4.10)	Name of organisation	O = German Federal Chamber of Notaries

organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Body
commonName (2.5.4.3)	Name holder	CN = BNotK Root CA 2017
Validity		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Start	Start certificate validity
	End	End of certificate validity
Holder		
countryName (2.5.4.6)	Name country holder	C = DE
organizationName (2.5.4.10)	Name of organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Body
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK qSig CA 2017
Extensions		
keyUsage (2.5.29.15)	Purpose	keyCertSign, cRLSign
basicConstraints (2.5.29.19)	Restrictions on the use of the certificate	Type applicant=Certification Body Constraint path length=0
subjectKeyIdentifier (2.5.29.14)	Public key identifier of the holder	e.g. [CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Issuer public key identifier	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Reference to issuer and service for status inquiry	see following elements

calssuers (1.3.6.1.5.5.7.48.2)	URL to exhibitor info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL to the OCSP service	http://ocsp.zs.bnotk.de/eqsig

► Sub-CA Certificate Profile ECC

Field (OID)	Description	Value
Version	x.509 version number	V3 (2)
serialNumber (2.5.4.5)	serialNumber of the certificate	e.g. [6f b8 e3 d6 dc a1 f6 bb]
Signature algorithm (1.2.840.10045.4.3.4)	Identifier (OID) Signature algorithm	SHA512WITHECDS
Key length	Key length	521 bits
Issuer		
countryName (2.5.4.6)	Name country issuer	C = DE
organizationName (2.5.4.10)	Name of organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Body
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK Root CA 2017
Validity		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Start	Start certificate validity
	End	End of certificate validity
Holder		
countryName (2.5.4.6)	Name country holder	C = DE

organizationName (2.5.4.10)	Name of organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Body
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK qSig CA 2017
Extensions		
keyUsage (2.5.29.15)	Purpose	keyCertSign, cRLSign
basicConstraints (2.5.29.19)	Restrictions on the use of the certificate	Type applicant=Certification Body Constraint path length=0
subjectKeyIdentifier (2.5.29.14)	Public key identifier of the holder	e.g. [CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Issuer public key identifier	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Reference to issuer and service for status inquiry	see following elements
calssuers (1.3.6.1.5.5.7.48.2)	URL to exhibitor info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL to the OCSP service	http://ocsp.zs.bnotk.de/eqsig

7.1.2 Participant certificate profile

► RSA

Field (OID)	Description	Value
Version	x.509 version number	V3 (2)
serialNumber (2.5.4.5)	serialNumber of the certificate	e.g. [6f b8 e3 d6 dc a1 f6 bb]
Signature algorithm	Identifier (OID) Signature algorithm	SHA512withRSAandMGF1 (1.2.840.113549.1.1.10)
Signature hash algorithm	Identifier (OID)	SHA-512

	Signature hash algorithm	(2.16.840.1.101.3.4.2.3)
algorithmIdentifier	Identifier (OID) key algorithm	RSA (1.2.840.113549.1.1.1)
Key length	Key length	2048 bits
Issuer		
countryName (2.5.4.6)	Name country issuer	C = DE
organizationName (2.5.4.10)	Name of organisation	O = German Federal Chamber of Notaries
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = Certification Body
commonName (2.5.4.3)	Name holder	e.g. CN = BNotK qSig CA 2017
Validity		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Start	Start certificate validity
	End	End of certificate validity
Holder		
countryName (2.5.4.6)	Name country holder	e.g. C = DE Country in which the certificate holder resides or in which the presented identification document of the certificate holder was issued.
organizationName (2.5.4.10)	Name of organisation	O = [Organisation]
organizationIdentifier (2.5.4.97)	Identification organisation	2.5.4.97 = [Identifier Organisation]
organizationalUnitName (2.5.4.11)	Name organisational unit	OU = [Department]
commonName (2.5.4.3)	Name holder	CN = First name(s) Last name
serialNumber (2.5.4.5)	Identifier holder	2.5.4.5 = Identification number (locally defined, if applicable)

givenName (2.5.4.42)	First name holder	2.5.4.42 = First name(s)
surname (2.5.4.4)	Surname holder	2.5.4.4 = Surname
title (2.5.4.12)	Title holder	2.5.4.12 = Title
emailAdress (1.2.840.113549.1.9.1)	Email address holder	emailAdress = [name@domain.tld]
userID (0.9.2342.19200300.100.1.1)	Unique user ID for linking means of authentication and remote signature	restrictedID of the eID, unique user ID of card owner
Extensions		
keyUsage (2.5.29.15)	Purpose	nonRepudiation
basicConstraints (2.5.29.19)	Restrictions on the use of the certificate	Type applicant=End Entity Restriction path length=None
subjectKeyIdentifier (2.5.29.14)	Public key identifier of the holder	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Issuer public key identifier	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Reference to issuer and service for status inquiry	see following elements
calssuers (1.3.6.1.5.5.7.48.2)	URL to exhibitor info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL to the OCSP service	http://ocsp.zs.bnotk.de/eqsig
CertificatePolicies (2.5.29.32)	Reference to applicable certification policy	see following elements
Policy information	policyIdentifier	Identifier (OID) and URL reference to CP 1.3.6.1.4.1.41460.5.1.1.1.2
	policyQualifier	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
Policy information	policyIdentifier	Identifier (OID) and URL reference to CPS 1.3.6.1.4.1.41460.5.2.1.1.2

	policyQualifier		https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
Policy information	policyIdentifier	Identifier (OID) and URL reference to PDS	1.3.6.1.4.1.41460.5.3.1.1.2
	policyQualifier		https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
qcStatements (1.3.6.1.5.5.7.1.3)		Identifier (OID) eIDAS compliance qSig	see following elements
QcCompliance (0.4.0.1862.1.1)		Qualified certificate	0.4.0.1862.1.1
QcSSCD (0.4.0.1862.1.4)		Generation on SSCD	0.4.0.1862.1.4
QcType (0.4.0.1862.1.6)		Type (Electr. signature)	0.4.0.1862.1.6.1
QcPDS (0.4.0.1862.1.5)		URL reference to PDS	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
subjectAltName (2.5.29.17)		Email address holder	[name@domain.tld]
Subject Directory Attributes (2.5.29.9)		Additional features describing the holder or certificate	see following elements
dateOfCertGen (1.3.36.8.3.1)		Date of certificate creation	e.g. 2017-10-09 08:57:57 UTC
For signature cards: integratedCircuitCard SerialNumber (1.3.36.8.3.6)		Unique identification of the SSCD	[VDA-specific ID]
admission (1.3.36.8.3.3)		Occupational attributes holder	[admissionAuthority, namingAuthority, professionInfo]
procuration (1.3.36.8.3.2)		Information on procuration	[StringType]
restriction (1.3.36.8.3.1)		Other restrictions related to the use of the certificate	[StringType]

7.2 Revocation list profiles

Revocation lists are not provided for qualified certificates.

7.3 Status query service profiles

An OCSP responder according to RFC 6960 is operated to query the status of the certificates, which also supports positive information (certHash extension). The responses of the OCSP responder are signed in a qualified manner.

The BNotK OCSP responder provides information on the validity of a certificate at a specific time for a requesting third party. The following statuses are returned:

- ▶ good – the certificate exists in the directory service and is not revoked,
- ▶ unknown – the certificate does not exist in the directory service,
- ▶ revoked – the certificate was revoked at the specified time.

8 Compliance check

See section 8 of the Certificate Policy (CP) of the VDA BNotK.

9 Other business and legal regulations

See section 9 of the Certificate Policy (CP) of the VDA BNotK.

<https://zertifizierungsstelle.bnotk.de/>

